

Title: Matrices: A Secret Weapon

A participatory lesson exploring the use of matrices in cryptology.

Link to Outcomes:

- **Problem Solving** Students will use more than one approach to solve problems involving cryptography and cryptanalysis.
- **Communication** Students will discuss coding concepts with other students. They will create and decipher original codes.
- **Reasoning** Students will make and test conjectures. They will formulate logical arguments and counter examples based upon the rules of the English language.
- **Connections** Students will explore the link between mathematical coding and English grammar.
- **Algebra** Students will use tables as tools to decipher codes.
- **Statistics** Students will construct and draw inferences from charts that summarize data from real-world situations.
- **Probability** Students will use experimental and theoretical distributions to solve problems involving codes. They will create and interpret probability distributions.
- **Discrete Math** Students will develop and analyze algorithms. They will investigate the connection between computers and the application of coding algorithms.
- **Cooperation** Students will demonstrate the ability to work as a member of a team in problem solving situations.

Brief Overview:

Many students have a fascination with secret messages. This lesson uses matrices and modular mathematics to explore the encoding and decoding of such messages. Students will investigate methods of coding, which include shift transformations, keyword codes, and polygraphic systems. Students will be able to encipher and decipher messages using these methods. Students will discover the importance of matrices and their application to cryptology. For the lower level courses, this lesson could be an exploratory activity not only for Cryptology but for the math content (matrices). For the higher level courses, this lesson could help students discover the complex mathematical basis and apply their mathematical knowledge of matrices to both Cryptography and Cryptanalysis.

Grade/Level:

Grades 9-12: Algebra I - Calculus

Duration/Length:

This lesson is expected to take a minimum of four days.

Prerequisite Knowledge:

Students should be familiar with matrix operations on the graphing calculator. The program MODULO, included in the lesson, is written specifically for the TI-82 graphics calculator.

Objectives:

Students will:

- encode and decode messages using shift transformations.
- encode and decode messages using keyword methods.
- encode and decode messages using polygraphic systems.
- construct and analyze frequency distributions.
- become proficient at using the graphing calculator for matrix operations.
- program a graphing calculator.
- use syntactical patterns of the English language.

Materials/Resources/Printed Materials:

- Graphics Calculator (TI-82 preferred)
- Teacher Aids
- Student Worksheets
- Additional Resources

Development/Procedure:

Students should be in groups of two for the entire lesson. Each student should have access to a graphing calculator. In addition to mathematical ability, encoding and decoding messages requires patience, insight, and even a little bit of luck. Therefore, students should be encouraged to exchange ideas and strategies.

Activity 1: Shift Transformations

- Warm-Up; Students will attempt to decode a message that is on the board or overhead. (Teacher Aid #1)

- Discuss the use of codes in transmission, the transmission of messages, computer security, and other topics which the students generate. (Teacher Aid #2)
- Through class discussion and student suggestions, decipher the Warm-Up. Help students formalize the methods used to decode the message. Use standard sequence and cipher to facilitate discussion. (Teacher Aid #3)
- Allow students to work together to decode Worksheet #1. Upon completion of the activity, the teacher should lead a discussion about shift transformations and the Caesar Cipher. (Teacher Aid #4)
- Students should use a shift transformation of their choice to encode a message for their partner to decode.
- After practicing with the codes they have created, the students should complete Worksheet #2. This worksheet contains two messages which were encoded using a method other than shift transformation.

Activity 2: Frequency Distributions

Students should discover that not all messages are encoded using shift transformations.

- Discuss the ease of decoding shift transformations and the necessity of using other types of coding methods.
- Compare shift transformation decoding methods with methods which might be used to decode #2 and #5 on Worksheet #2. This will prompt discussion of the use of frequency tables. (Teacher Aid #5)
- Use frequency distribution tables to decode #2 and #5 from Worksheet #2.
- Introduce the concept of keyword codes. (Teacher Aid #6, Methods I and II)
- Students should practice creating keyword ciphers using Worksheet #3.

Activity 3: Keywords

- Warm-Up: Give students a message to encode with the cipher they created on Worksheet #3.
- Ask the students to exchange papers and decode the message. (Since they already know the message, this will not take very long.) Challenge the students to compare the cipher with the standard sequence to determine the key word.

- Discuss the relative ease of discovering the keyword after the code has been broken.
- Introduce the use of a keyword and a setting word. (Teacher Aid #6, Method III)
- Have students complete Worksheet #4.
- Review the use of the TI-82 matrix operations which will be used to encode and decode messages using the Polygraphic System.
- Practice matrix operations.
- Discuss modular math. (Teacher Aid #7)

Activity 4: Polygraphic Systems

- Warm-Up: Use the MODULO math formula to reduce each element in a given matrix to Mod 29. (Teacher Aid #8)
- Work through an example of encoding and decoding a message using the trigraph system. (Teacher Aid #9 and Worksheet #6)
- Discuss the arbitrary choice of the coding matrix. Emphasize that the number of symbols to be encoded must be a multiple of n (for an $n \times n$ code matrix). Spaces should be added to the end of the message if the number of characters in your message is not a multiple of n .
- Complete Worksheet #7

Evaluation:

Evaluation will be based upon group discussions, creativity, and initiative. Worksheets may be collected. Formal assessment will include encoding and decoding messages as well as knowledge of cryptologic methods. Research papers on cryptology, methods of enciphering and deciphering codes, modern use of codes, or mathematicians who have been involved with these topics should also be considered. These papers will help students realize that mathematics is a dynamic subject which continues to evolve.

Extensions:

- Affine Transformations
- Public Key Cryptology
- Symbolic Code

Authors:

Christine M. Forester
Park View High School
Loudoun County

Christine A. Rivecco
Mount Vernon High School
Fairfax County

Vocabulary List

cipher sequence
coding matrix
cryptanalysis
cryptography
cryptology
decipher
decoding matrix
digraphic
encipher
frequency distribution
keyword
modular mathematics
plain sequence
plain text matrix
polygraphic system
setting word
shift transformation
trigraphic

Teacher Aid #1: Activity 1 Warm-Up

Warm-Up Discover the hidden message!

RFC ZPGRGQF YPC AMKGLE

Teacher Aid #2 Historical Perspective

Secret codes are almost as old as writing itself. The Persians were the first known “cryptographers.” The word cipher (a system of secret writing based upon a key) comes from the Arabic word SIFR. Secret codes have been used in almost every war. Sometime with disastrous results. Today, computers are used to create sophisticated codes.

Sir Harry Ordway was a double agent who delivered this message:

“Sir Harry Ordway Often Tells Things Hopeful In Solving Movements Artillery. Necessary Arrange Terms Of New Compensation Employment.”

Why was he upset?

The study of secret codes is referred to as Cryptology. Cryptography is the process of writing (enciphering) code and cryptanalysis is the science used to crack a code (decipher).

Cryptology is a fascinating topic which can be explored at a very elementary level requiring very little mathematical background. However, further exploration will reveal the complex mathematical basis of both cryptography and cryptanalysis. At any level, cryptanalysis involves perseverance, insight, and even a bit of luck.

Teacher Aid #3: Hints to Decode Messages

- Write the letters of the alphabet in order. This is called the plain sequence. As you discover the character from the coded message that matches the letter in the plain sequence, write the character below the letter it matches. This list will become the cipher used to encode the message.
- Write the coded message in large letters and as soon as you find the meaning of a code letter, write it beneath the code-letter all through the message.
- Try to find vowels because every word has at least one. Look for one-letter words which must be A or I. Double letters might be OO or EE (the most common double vowels). Another common pair of letters is TH. The most common 3 letter group (as a word or as a part of a word) is THE.
- Punctuation marks help the code breaker. They are not usually included in a secret message, but if they are, look for the following patterns:
 - a. The words OR, AND, and BUT often come after commas.
 - b. THAT, WHO, and WHICH often come before commas.
 - c. A sentence with a ? often begins with W.
- If you suspect that the code is a simple shift transformation, choose a group of characters and list the alphabetic characters beneath them. You will find a that a word is formed and you will be able to break the code.

ex. the message is **MJQQT**

nkrru
olssv
pmttw
qnuux
rovvy
spwwz
tqxxa
uryyb
vszzc
wtaad
xubbe
yvccf
zwddg
axeeh
byffi
czggj
dahhk
ebiil
fcjjm
gdkkn
hello

Teacher Aid #4: Shift Transformations

The cipher obtained by adding a number to the alphabetic position number of the standard sequence is called a shift transformation. The value of the added integer is the shift factor.

For example: The position number of the letter “e” is 5. If we add 2 to the position number we get 7 which means that in our code all letters will be shifted two positions to the right and an “e” in our message will appear as an “g” in our code.

Standard sequence:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Cipher Sequence:

Y Z A B C D E F G H I J K L M N O P Q R S T U V W X

Message: HELLO

Cipher: FCJJM

In this example, our cipher is a shift transformation and our shift factor is 2.

The cipher obtained by adding **3** to the plain sequence is referred to as the Caesar Cipher. Julius Caesar used this technique on the Roman Alphabet.

The Vigenere Table

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Plain————→	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher																										
0	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r
19	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Teacher Aid #5: Frequency Distributions

Frequency count for letters in a passage containing 100 letters

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	1	3	4	13	3	2	4	7	0	0	4	3	8	7	3	0	8	6	9	3	1	2	0	2	0

When decoding a message, it is often helpful to count the occurrences of the characters and compare your count with the frequency table. This will allow you to make some “educated” guesses when trying to decipher the messages.

Teacher Aid #6: Keywords - Method I

A cipher can be created by using a keyword.

For example, if we choose “statistic” as our keyword, our cipher would be determined as follows:

Method I.

Write the word “statistic” without the repeated letters. Then complete the cipher with the unused alphabet characters.

Standard sequence:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher sequence:

S T A I C B D E F G H J K L M N O P Q R U V W X Y Z

In this case, the message HELLO becomes ECJJM.

Comparing the standard sequence to the cipher sequence you find that the letters U through Z are the same in both sequences. The number of letters which remain the same will depend upon the choice of the keyword. This can be avoided by using Method II.

Teacher Aid #6: Keywords - Method II

Method II.

Using the same keyword “statistic,” another cipher can be created by writing it without its repeated letters and then writing the remaining alphabetical characters beneath the letters.

S	T	A	I	C
B	D	E	F	G
H	J	K	L	M
N	O	P	Q	R
U	V	W	X	Y
Z				

The cipher will be created by reading the table vertically and matching the letters to the standard sequence.

Standard sequence:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher sequence:

S B H N U Z T D J O V A E K P W I F L Q X C G M R Y

Our message HELLO becomes DUAAP.

A comparison of the standard sequence with the cipher sequence reveals that none of the characters are the same. Using Method II does not guarantee that there will be no matches, however, it does provide a better scrambled cipher than Method I.

Teacher Aid # 6: Keywords - Method III

Method III.

The use of the first two methods results in one cipher for each keyword which is chosen. This type of code becomes relatively easy to break once the keyword is discovered. The use of a keyword and a setting word will generate multiple ciphers depending upon the number of characters in the setting word.

For example, keeping our keyword as “statistic” and using “mode” as our setting word, the ciphers can be created as follows:

Using Method I, create the cipher

Standard sequence:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher sequence:

S T A I C B D E F G H J K L M N O P Q R U V W X Y Z

Using the letters of the setting word as the first character of the ciphers, four additional ciphers can be created.

Cipher 1

M N O P Q R U V W X Y Z S T A I C B D E F G H J K L

Cipher 2

O P Q R U V W X Y Z S T A I C B D E F G H J K L M N

Cipher 3

D E F G H J K L M N O P Q R U V W X Y Z S T A I C B

Cipher 4

E F G H J K L M N O P Q R U V W X Y Z S T A I C B D

Message: HELLO

Cipher 1: VQZZA Cipher 2: XUTTC

Cipher 3: LHPPU Cipher 4: MJQQV

Therefore, a message could be encoded using any one of the ciphers or a combination of the ciphers to make decoding by anyone but the intended receiver more difficult.

Teacher Aid #7: Modular Mathematics

Modular mathematics, often referred to as “clock arithmetic.”
The mod is the remainder when a number is divided by a set number.

For example:

$$135 \bmod 36 = 27$$

the remainder after you divide 135 by 36 is 27.

Mathematically:

$$135/36 = 3.75$$

Multiply the decimal portion of your answer by the divisor to obtain the integer value of the remainder:

$$.75 \times 36 = 27$$

Teacher Aid #8: Activity 4 Warm-Up

Reduce the following matrix to mod 29. (Use the program on your calculator from last night's homework.)

Place matrix in [A]

$$\begin{bmatrix} 245 & 131 & 125 \\ 45 & 87 & 156 \\ 89 & 46 & 35 \end{bmatrix} \begin{bmatrix} 113 & 15 & 9 \\ 16 & 0 & 11 \\ 2 & 17 & 11 \end{bmatrix}$$

On the TI-82 the formula to store matrix [A] MOD 29 in matrix [D] is:

$$((\text{fPart}([A] * (1/29))) * 29) \rightarrow [D]$$

On the TI-82 the sequence is:

```
((  
MATH  
→NUM  
3 [fPart]  
MATRIX  
[A]  
*  
(  
1  
÷  
29  
)))  
*  
29  
)  
STO→  
MATRIX  
[D]
```

Teacher Aid #9: Polygraphic Systems

Shift transformations and the keyword method of coding are substitution ciphers. A substitution cipher always uses the same character to replace a particular letter in the plain sequence. For example if the letter “e” in the coded message represents the letter “s” in the plain sequence, then every time an “e” is encountered in the coded message, it will be replaced by the letter “s.” Therefore, substitution ciphers are easily decoded using frequency distributions of single letters and letter combinations.

Polygraphic systems encode a group of plain sequence letters. This scrambles the frequencies and allows for more than one representation of a plain sequence character. The digraphic system is the simplest polygraphic system. It uses a 2 x 2 coding matrix to replace pairs of plain sequence characters. A square matrix of any size may be chosen as a coding matrix. The larger the coding matrix the more complex the system of cryptography.

The examples in this unit use a trigraphic system. A 3 x 3 matrix is chosen as the coding matrix. The choice of the matrix is arbitrary. The only constraint is that the coding matrix must have an inverse. It is convenient to have a prime number of characters in the plain sequence. Therefore, we have added a space and two punctuation marks to the standard alphabet to create our plain sequence. The plain sequence and its numerical representations are:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P	Q	R	S	T	U	V	W	X	Y	Z		?	!	
16	17	18	19	20	21	22	23	24	25	26	27	28	29	

Teacher Aid #9: Polygraphic Systems (continued)

For the message, “Imagination is more important than knowledge,” we will encode groups of three letters. This system is called **trigraphing**.

TO ENCODE A MESSAGE...

First, choose a coding matrix. (Be sure the matrix is 3x3 and has an inverse.)

$$\begin{bmatrix} 6 & 5 & 2 \\ 5 & 5 & 2 \\ 2 & 2 & 1 \end{bmatrix}$$

Second, assign plain text numbers to letters in the message.

I M A G I N A T I O N I S M O R E I M P O R T A N T
9 13 1 7 9 14 1 20 9 15 14 9 19 13 15 18 5 9 13 16 15 18 20 1 14 20

T H A N K N O W L E D G E
20 8 1 14 11 14 15 23 12 5 4 7 5

Third, place the numbers vertically in a matrix with **three** rows. We will call this the plain text matrix. (It is important that you take the numbers in multiples of three.)

$$\begin{bmatrix} 9 & 7 & 1 & 15 & 19 \\ 13 & 9 & 20 & 14 & 13 \\ 1 & 14 & 9 & 9 & 15 \end{bmatrix}$$

Fourth, multiply the plain text matrix by the coding matrix to **encode** the message.

$$\begin{bmatrix} 6 & 5 & 2 \\ 5 & 5 & 2 \\ 2 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 9 & 7 & 1 & 15 & 19 \\ 13 & 9 & 20 & 14 & 13 \\ 1 & 14 & 9 & 9 & 15 \end{bmatrix} = \begin{bmatrix} 121 & 115 & 34 & 178 & 209 \\ 112 & 108 & 33 & 163 & 190 \\ 45 & 46 & 15 & 67 & 79 \end{bmatrix} *$$

*If using the formula on the next page, this matrix should be stored in [A].

Next, reduce each element of the resulting matrix to mod 29. Use the formula:

$$((\text{fPART}([A]*(1/29))) * 29 \rightarrow [D])$$

$$\begin{bmatrix} 5 & 28 & 5 & 4 & 6 \\ 25 & 21 & 4 & 18 & 16 \\ 16 & 17 & 15 & 9 & 21 \end{bmatrix}$$

Finally, reassign letters and symbols to the numbers in the matrix for transmission of the message.

$$\begin{bmatrix} 5 & 28 & 5 & 4 & 6 \\ 25 & 21 & 4 & 18 & 16 \\ 16 & 17 & 15 & 9 & 21 \end{bmatrix} \Rightarrow \begin{bmatrix} E & ? & E & D & F \\ Y & U & D & R & P \\ P & Q & O & I & U \end{bmatrix}$$

Message to send: EYP?UQEDODRIFPU

*Remember, this is only the first 15 letters of the message. Use the space below to encode the remaining letters.

MESSAGE RECEIVED: **EYP?UQEDODRIFPU**

To DECIPHER this message...

First, assign a plain text number to each symbol in the message.

E	Y	P	?	U	Q	E	D	O	D	R	I	F	P	U
5	25	16	28	21	17	5	4	15	4	18	9	6	16	21

Second, place numbers in a 3x5 matrix. We will call this the cipher text matrix.

$$\begin{bmatrix} 5 & 28 & 5 & 4 & 6 \\ 25 & 21 & 4 & 18 & 16 \\ 16 & 17 & 15 & 9 & 21 \end{bmatrix}$$

Third, find the inverse of the **coding matrix**. We will call this the **decoding matrix**.

$$\begin{bmatrix} 1 & -1 & 0 \\ -1 & 2 & -2 \\ 0 & -2 & 5 \end{bmatrix}$$

Next, multiply the cipher text matrix by the **decoding matrix**.

$$\begin{bmatrix} 5 & 28 & 5 & 4 & 6 \\ 25 & 21 & 4 & 18 & 16 \\ 16 & 17 & 15 & 9 & 21 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 & 0 \\ -1 & 2 & -2 \\ 0 & -2 & 5 \end{bmatrix} = \begin{bmatrix} 9 & 7 & 1 & 15 & 19 \\ 13 & 9 & 20 & 14 & 13 \\ 1 & 14 & 9 & 9 & 15 \end{bmatrix}$$

Finally, reassign plain text letters to the numbers in the resulting matrix.

$$\begin{bmatrix} 9 & 7 & 1 & 15 & 19 \\ 13 & 9 & 20 & 14 & 13 \\ 1 & 14 & 9 & 9 & 15 \end{bmatrix} \Rightarrow \begin{bmatrix} I & G & A & O & S \\ M & I & T & N & M \\ A & N & I & I & O \end{bmatrix}$$

Decoded message: IMAGINATIONISMO

*Again, these are only the first fifteen letters of the message. Decode the remaining symbols on another sheet of paper.

Name _____

WORKSHEET #1

Decipher each message written in code.

1. TE DEJ FQII WE

Message:

Standard sequence:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher:

2. OTBGJKCGYNOTMZUTGZJGCN

Message:

Standard sequence:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher:

3. HFVATZNGUGBOERNXFRPERGPBQRFVFSHA

Message:

Standard sequence:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher:

4. QGM SAFL FGLZAF TML S ZGMFV VGY

Message:

Standard sequence:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher:

5. Explain how you deciphered these codes. Include in your discussion any patterns you noticed between the standard sequence and the cipher.

Name _____

WORKSHEET #2

Decipher each message written in code.

1. CPLOPXTTFDSFUDPEFT

Message:

2. MCFJ XUT FJ MGFNLB

Message:

3. IQOYJYIDJIE

Message:

4. LPJOD ODZ MVQZI IZQZMHJMZ

Message:

5. QMODQAUMOIHKCHIQAY

Message:

Name _____

WORKSHEET #3

Keyword codes

1. Use the keywords CRYPTOGRAPHY and UNIVERSITY to write two cipher alphabets.

Standard:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher 1:

Cipher 2:

2. Use each cipher to encode the message "The Eagle has landed"

Coded message using cipher 1:

Coded message using cipher 2:

3. Choose your own code word, and write its cipher alphabet.

Code word:

Cipher:

4. Encode a message for your partner to solve.

Name_____

WORKSHEET #4

Keywords and Setting Words

1. Create the ciphers that result if you choose “pharmacology” as your keyword and “diet” as your setting word.

2. How many ciphers did you create?

3. Using the ciphers that were created in number 1, encode the following message:

IF YOU WANT TO KNOW THE TRUE CHARACTER OF A PERSON DIVIDE AN
INHERITANCE WITH HIM

4. Choose a keyword and a setting word and create the ciphers that would result from your choice.

Name _____

WORKSHEET #5

Review of matrices

Enter the following matrices into your calculator and perform the indicated operations.

$$1. \quad \begin{bmatrix} 1 & 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 4 & 5 \\ 6 & 7 \\ 8 & 9 \end{bmatrix}$$

$$2. \quad \begin{bmatrix} 2 & 1 \\ 0 & 8 \end{bmatrix} \cdot \begin{bmatrix} -5 & 11 & 7 \\ 1 & 0 & 1 \\ 13 & 8 & 9 \end{bmatrix}$$

$$3. \quad \begin{bmatrix} 15 & 1 & 13 & 3 \\ 2 & 14 & 4 & 12 \\ 11 & 5 & 9 & 7 \\ 6 & 10 & 8 & 0 \end{bmatrix}^2$$

Use your calculator to find the inverse of each matrix.

$$4. \quad \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$$

$$5. \quad \begin{bmatrix} 6 & -8 \\ -3 & 4 \end{bmatrix}$$

$$6. \quad \begin{bmatrix} 1/2 & -1/2 & 1/2 \\ -1 & 1 & 0 \\ -1/2 & 3/2 & -1/2 \end{bmatrix}$$

Name _____

WORKSHEET #6

Polygraphic Systems

For the message, “Imagination is more important than knowledge,” we will encode groups of three letters. This system is called **trigraphing**.

TO ENCODE A MESSAGE...

First, choose a coding matrix. (Be sure the matrix is 3x3 and has an inverse.)

$$\begin{bmatrix} 6 & 5 & 2 \\ 5 & 5 & 2 \\ 2 & 2 & 1 \end{bmatrix}$$

Second, assign plaintext numbers to letters in the message.

I--M--A--G--I--N--A--T--I--O--N--I--S--M--O--R--E--I--M--P--O--R--T--A--N--T

T--H--A--N--K--N--O--W--L--E--D--G--E

Third, place the numbers vertically in a matrix with **three** rows. (It is important that you take the numbers in multiples of three.)

Fourth, multiply the text matrix by the coding matrix to **encode** the message.

Next, reduce each element of the resulting matrix to mod 29. (Use the program on your calculator, which you programmed last night.)

Finally, reassign letters and symbols to the numbers in the matrix for transmission of the message.

\Rightarrow

Message to send: EYP?UQEDODRIFPU

*Remember, these are only the first 15 letters of the message. Use the space below to encode the remaining letters.

MESSAGE RECEIVED: **EYP?UQEDODRIFPU**

To DECIPHER this message...

First, assign a plaintext number to each symbol in the message.

E--Y--P--?--U--Q--E--D--O--D--R--I--F--P--U

Second, place numbers in a 3x5 matrix.

Third, find the inverse of the **coding matrix**. We will call this the **decoding matrix**.

Next, multiply the text matrix by the **decoding matrix**.

Finally, reassign plaintext letters to the numbers in the resulting matrix.

==>

Decoded message: IMAGINATIONISMO

*Again, these are only the first fifteen letters of the message. Decode the remaining symbols on another sheet of paper.

Name_____

WORKSHEET #7

Polygraphic Systems

Use a trigraphic system and the given coding matrix to encode the message:

IF YOU ARE TOO BUSY TO LAUGH YOU ARE TOO BUSY

*Remember to use the alphabet which includes a space, an exclamation point, and a question mark.

Coding matrix:

$$\begin{bmatrix} 0 & 2 & 3 \\ 1 & 4 & 7 \\ 2 & 3 & 6 \end{bmatrix}$$

Worksheet #7 (continued)

Use a trigraphic system and the given coding matrix to decode the message:

HW FDIYYWDFB !GUIVOGKOTTZFCJYYKJ SILQ?U

*Remember to use the alphabet which includes a space, an exclamation point, and a question mark. Also remember the different procedures for **encoding** and **decoding** a message.

Coding matrix*.

$$\begin{bmatrix} 5 & 4 & 10 \\ 2 & 2 & 5 \\ 6 & 1 & 3 \end{bmatrix}$$

*If using the TI-82, check your encoding matrix and its inverse to make sure that the values work. 0 will be shown as a very small number in scientific notation. You can change the values to 0.

Additional Resources

Consortium for Mathematics and Its Applications, Inc. Modules: Tools for Teaching, COMAP, 1994.

Doubet, Farticant, Rockhill, Ryan. Advanced Mathematics. Prentice Hall: 1994.

Larson, Kanold, Stiff. Algebra 2. DC Heath: 1993.

Malkevitch, Joseph and Froelich, Gary and Froelich, Daniel. Codes Galore. COMAP: 1991.

Malkevitch, Joseph and Froelich, Gary. Loads of Codes. COMAP: 1993.

Rubenstein, Craine, Butts. Integrated Mathematics 2. McDougal-Littell: 1994.

Sinkov, Abraham. Elementary Cryptanalysis: A Mathematical Approach. The Mathematical Association of America. Washington D.C.: 1966.

ANSWER KEY

Teacher Aid #1: Warm-Up -- THE BRITISH ARE COMING

Teacher Aid #2: Historical Perspective

First letter of each word:

SHOOT THIS MAN AT ONCE!!

Teacher Aid #8: Warm-Up -- (MARTIX MOD 29)

Worksheet #1: Shift Transformations

1. DO NOT PASS GO
2. INVADE WASHINGTON AT DAWN
3. USING MATH TO BREAK SECRET CODES IS FUN
4. YOU AINT NOTHIN BUT A HOUND DOG

Worksheet #2: Shift Transformations

1. BO KNOWS SECRET CODES
2. THIS ONE IS TRICKY
3. SAY IT ISNT SO
4. QUOTH THE RAVEN NEVERMORE
5. I THINK THEREFORE I AM

Worksheet #3: Keyword codes

Cipher 1: CRYPTOGRAPBDEFIJKLMNQSUVWXZ

Cipher 2: UNIVERSTYABCDFGHJKLMOPQWXZ

Worksheet #4: Keywords and Setting Words

P H A R M C O L G Y B D E F I J K N Q S T U V W X Z

D E F I J K N Q S T U V W X Z P H A R M C O L G Y B

I J K N Q S T U V W X Z P H A R M C O L G Y B D E F

E F I J K N Q S T U V W X Z P H A R M C O L G Y B D

T U V W X Z P H A R M C O L G Y B D E F I J K N Q S